Computer Security. Extraordinary Evaluation Exam 2022-2023

Name:
UO:

NOTE: *This exam measures your ability to apply theoretical security knowledge at a particular time, and in your current circumstances. It measures neither your intelligence nor your overall ability. Trust yourself and go for it!, but if you have a bad day, better ones will come.* ***DO NOT let yourself down by a bad result***

1. ***The company I have joined has been attacked, and I have been given a log of connections that I am sure has not been altered. On the date and time of the attack there is a huge number of connections of the IP 192.168.10.15, and the IT manager of my company tells me that it is a Russian IP. Do you think it is possible that this IP is from Russia? Why? (1 point)***

2. ***My boss authorizes me to do a nmap scan to my company's network and I find an http service on the port 59345 of one of the machines. I asked, but no one knows what it does there or to whom it belongs. What do you think it may be a reason for the existence of this mysterious http service related to security? (1 point)***

3. ***Explain what I would have to do so that someone could send me encrypted messages that only I could read, based on the concepts of cryptography that we have seen in theory (1 point)***

Name:
UO:

4. ***How would you verify that a software you have downloaded has not been altered since its author published it (assume that the author provides you with the necessary data to do so, the question is regarding the procedure to verify it that you would follow) (1 point)***

5. ***An auditor has arrived to help us to implement ISO 27001 in our company, and you tell him that all the machines of the company have applied and verified all the security controls of the CIS Benchmarks corresponding to their OS. The auditor says that this is not useful to meet any criteria of the ISO 27001 standard, and that we have to start over. Is it true? Why? (1 point)***

6. ***You have been given this output and your boss says that it is impossible to determine if your Apache web server is vulnerable just with this information. Is he right? If not, how will you prove him wrong? (1 point)***

```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open     nping-echo Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

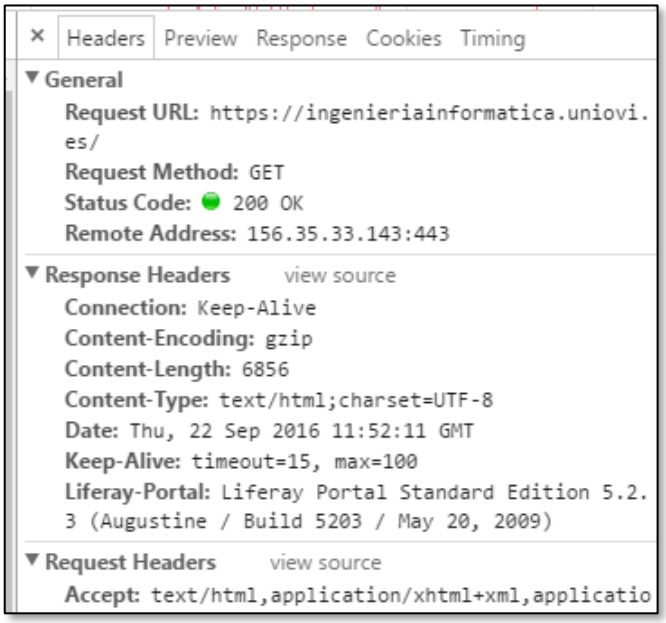
Name:
UO:

7. **Is there any type of application that can be used to test the application internal structures and source code for potential vulnerabilities or security problems prior to executing it?** ***(1 point)***

8. **Your boss says that with the new firewall blocking all incoming connections from untrusted places it is impossible to stablish any type of remote shell on the company machines. Is he right?** ***(1 point)***

Name:
UO:

9. **You have just located this into your browser development tools? What can you say about it? Can this facilitate locating security vulnerabilities? Does this website use CSP?** ***(1 point)***



10. **Can you explain what happened here? What should have the program do to prevent this?** ***(1 point)***